



新世代安全防禦思維

網路異常行為及威脅分析

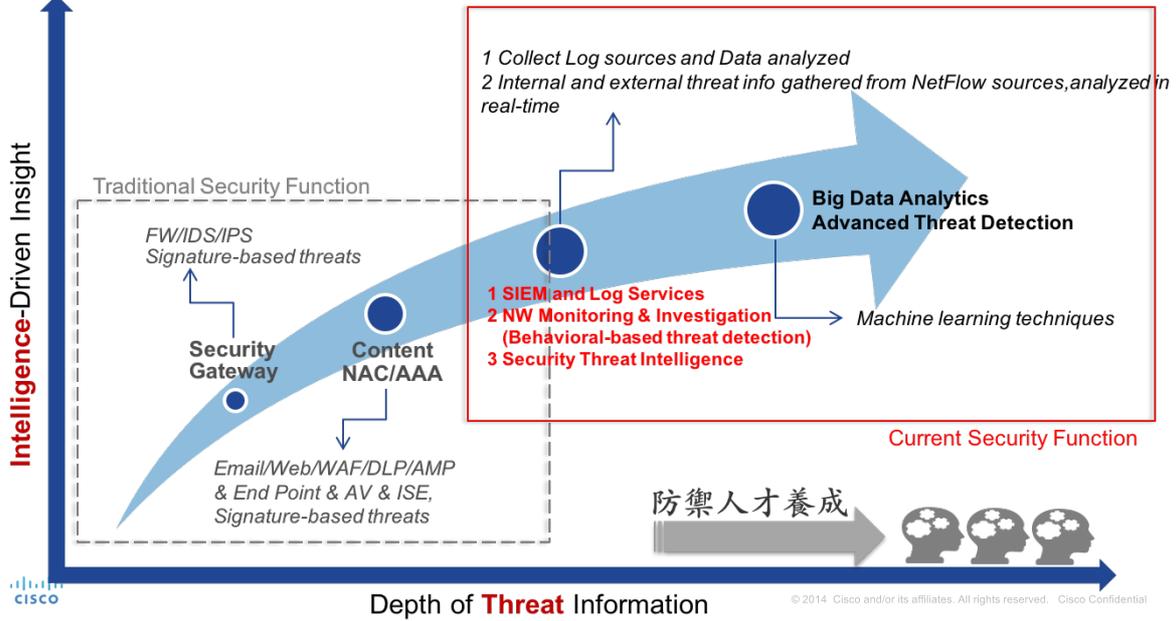
Allen Yu / 思科資安戰略暨資深顧問
Jan 26, 2018



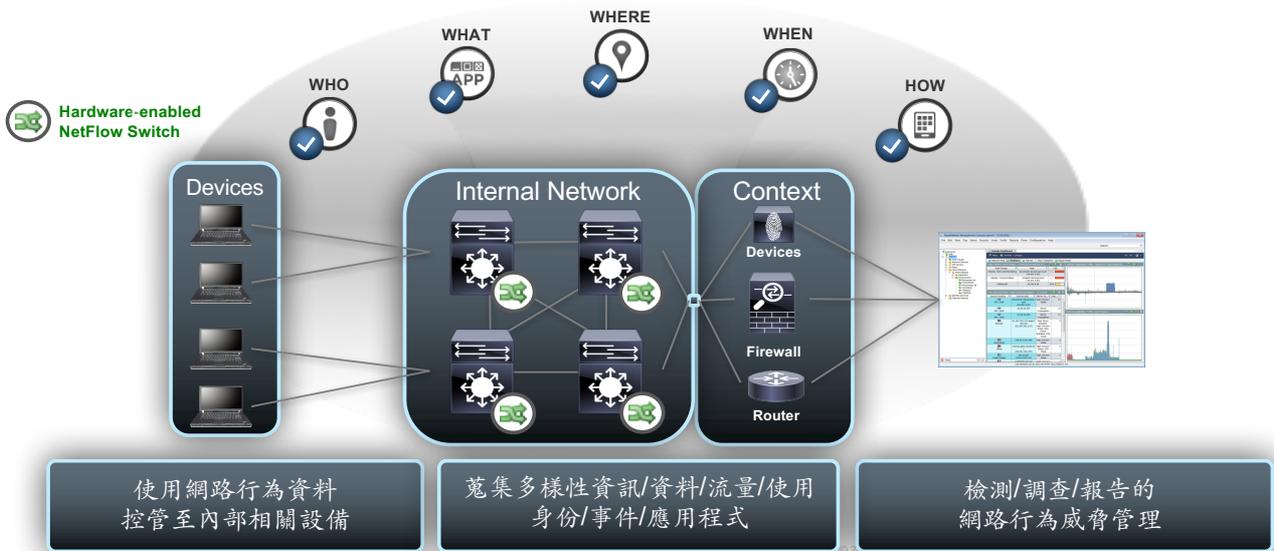
新世代安全防禦思維

— 智慧監測機制

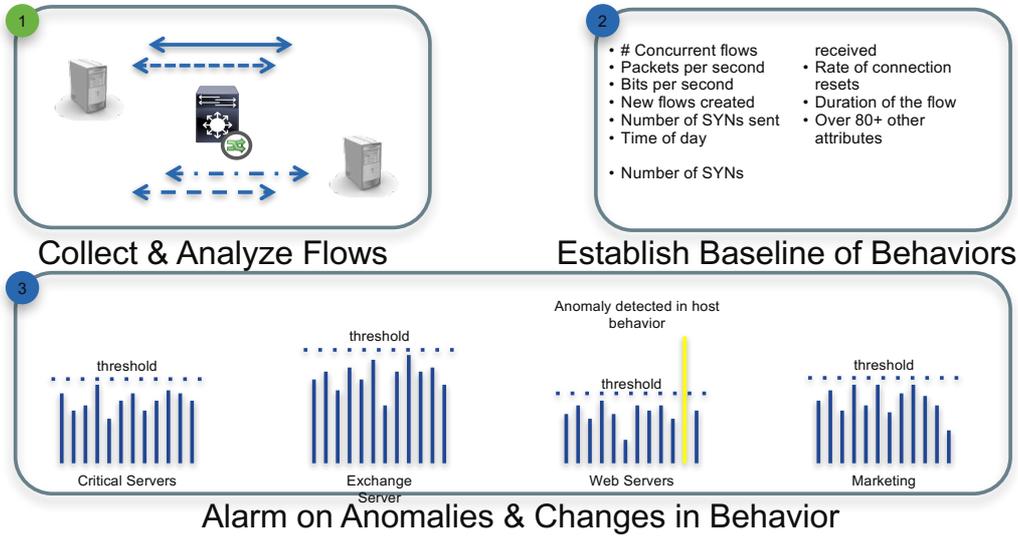
安全成熟度與防禦功能



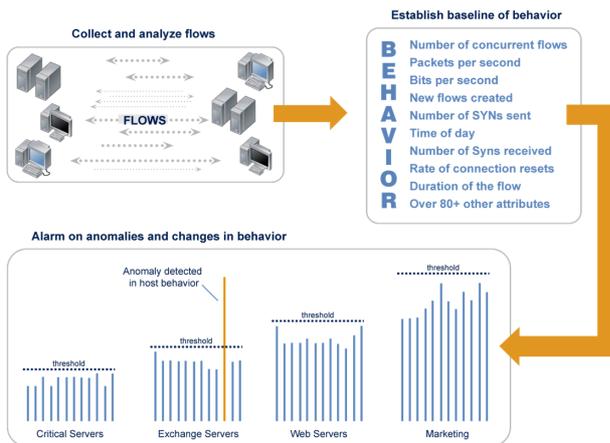
安全管理能見度(人/事/時/地/物)



安全行為異常檢測方法



BASELINING – 網路安全行為學習方法論

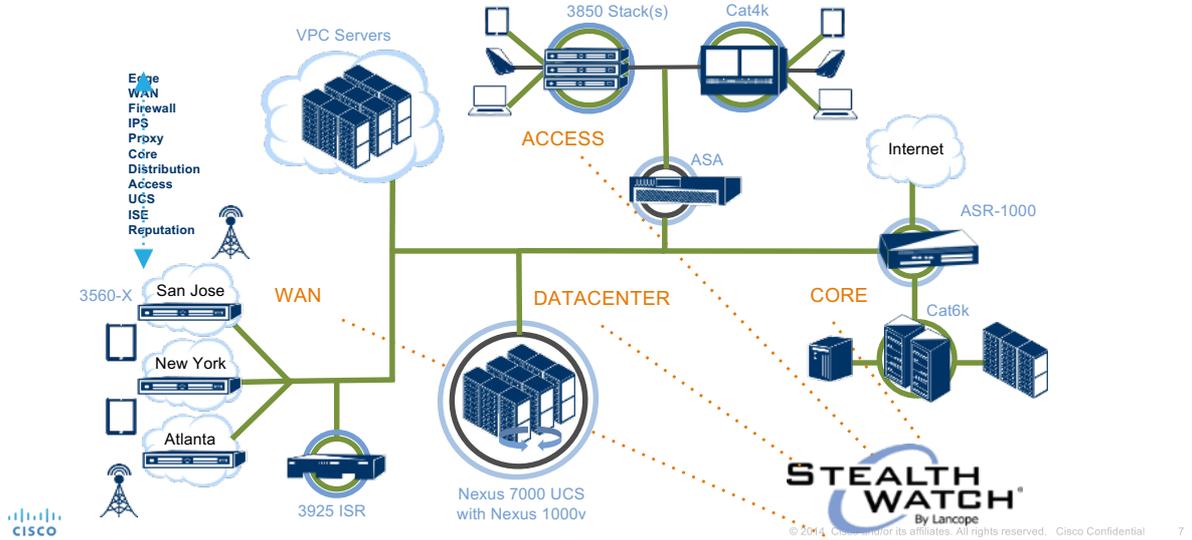


- 流量的內容/方向/大小量/時間
- 什麼是網路正常行為的設定檔
- 正常的網路行為屬性的基線
- 組織網路行為的學習與應用
- 網路行為基準線為基礎
- 進階式網路行為的監控及管理

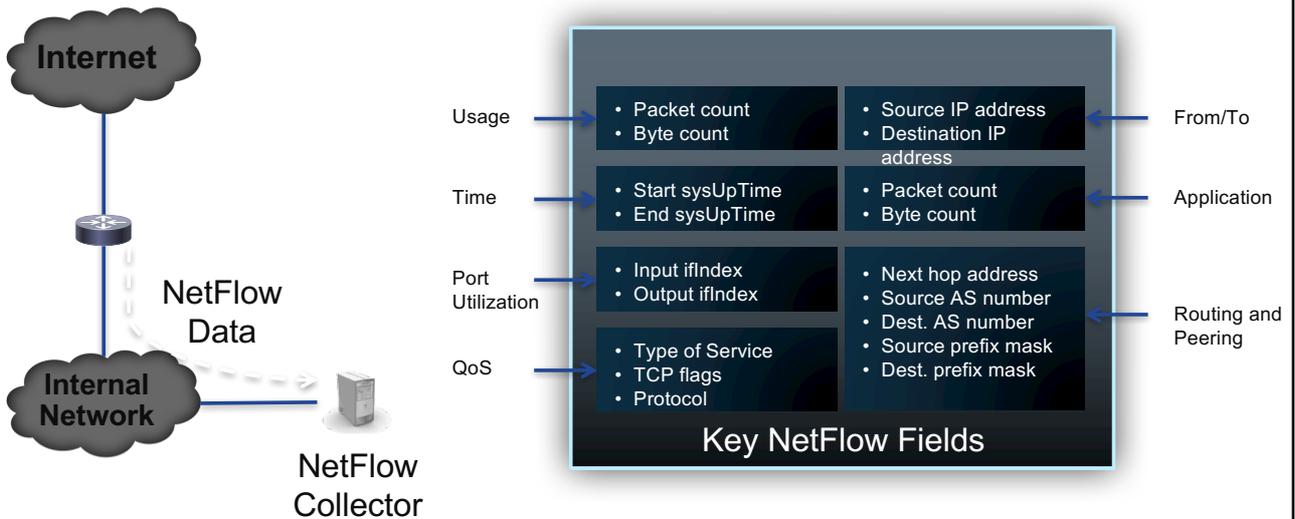


當你看不見攻擊的時候，肯定無法保護自己

Internal Visibility from Edge to Access, Network Is Your Sensor



Network as a Scalable Source of Truth



Conversational Flow Record

Start: 06/12 - 06:49:19 AM
End: 06/12 - 06:51:20 AM
Duration: 2m 1s

10.201.3.78
RFC 1918
ethel
14:7d:c5:bf:3:1:85
[View Details](#)

60173/TCP

11.72KB | 63 packets
→
HTTP
←
30.53KB | 45 packets

80/TCP

184.75.210.3
Canada

Who

What

How

Who

When

Where

More context

Flow Detailed Summary: 10.201.3.78

Search Subject Details	Totals	Peer Details
Packets: 63 Packet Rate: 0.52pps Bytes: 11.72KB Byte Rate: 99.15bps Percent Transfer: 27.7% Host Groups: Sales and Marketing, End User Devices, Atlanta Payload: GET http://www.acronymfinder.com/~rst/digg.gif	Packets: 108 Packet Rate: 0.89pps Bytes: 42.24KB Byte Rate: 357.48bps Search Subject/Peer Ratio: 0.38 TCP Connections: 12 RTT: 70ms SRT: 4ms	Packets: 45 Packet Rate: 0.37pps Bytes: 30.53KB Byte Rate: 258.33bps Percent Transfer: 72.3% Host Groups: Canada Payload: 200 OK

[Close](#)

Cisco Confidential 9

NetFlow 提供網路可視性



NetFlow provides

- Trace of every conversation in your network
- An ability to collect record **everywhere** in your network (switch, router, or firewall)
- Network usage measurement
- An ability to find **north-south** as well as **east-west** communication
- Light weight visibility compared to SPAN based traffic analysis
- Indications of Compromise (IOC)
- Security Group Information

Flow Information	Packets
SOURCE ADDRESS	10.1.8.3
DESTINATION ADDRESS	172.168.134.2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/0
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172.168.25.1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
APPLICATION NAME	NBAR SECURE-HTTP



網路異常行為分析 應用場景

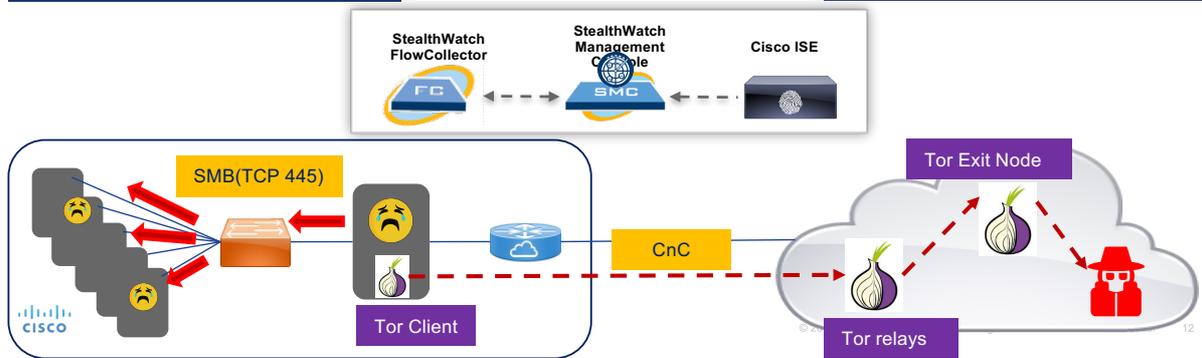
網路和安全視覺化報告	網路異常行為分析	安全威脅行為分析
<ul style="list-style-type: none"> 網路分段和主機分組 了解網路風險展示通訊狀態 高風險主機行為分析和統計 安全告警分類和趨勢分析 分析報告模版化、自動化 	<ul style="list-style-type: none"> 遠端存取和控制行為分析 異常或惡意的DNS活動分析 網路流量地域分佈異常分析 檢測隱秘流量出入情況 鑒定標準埠下的偽造應用連接 	<ul style="list-style-type: none"> 駭客掃描和探測攻擊分析 惡意代碼或蠕蟲擴散分析 敏感資料收集和資訊洩漏 DDOS攻擊分析 暴力破解密碼嘗試活動分析
稽核與合規分析	網路和應用性能分析	事件回應和調查取證
<ul style="list-style-type: none"> 檔案共用濫用合規分析 大量下載商務資料合規分析 業務節點之間網路、應用和服務存取合規性檢查 	<ul style="list-style-type: none"> 網路和應用狀態和傳輸分析 RTT統計分析和告警 SRT統計分析和告警 	<ul style="list-style-type: none"> 安全事件快速調查和追蹤，縮短回應時間 安全告警發送到協力廠商平臺聯合調查

CISCO

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 11

如何檢測勒索軟體

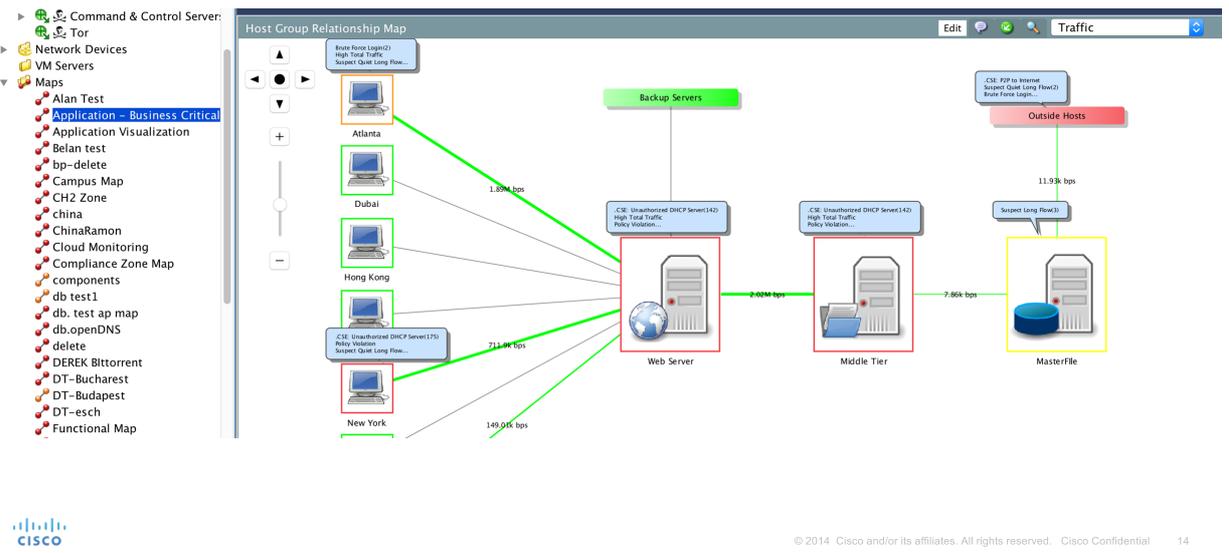
- | | | |
|---|--|--|
| <p>❖ 自動識別惡意程式的傳播</p> <ol style="list-style-type: none"> 1. 收集NetFlow資訊，機器學習分析 2. 發現基於SMB (TCP 445) 等高風險服務埠的掃描探測行為、大量異常連接和流量。 3. 自動追蹤惡意程式碼的傳播軌跡和影響範圍，調查源頭和途徑。 | <p>❖ 發現駭客的交互控制活動</p> <ol style="list-style-type: none"> 1. 安全智慧情報庫即時更新 (Talos 支持) 2. 即時更新Tor節點資訊，可以成功檢測Tor匿名活動和Bogon IP連接 3. 即時更新CnC資訊，可以成功檢測CnC駭客控制活動和連接 | <p>❖ 關聯分析和聯動緩解風險</p> <ol style="list-style-type: none"> 1. 基於業務主機和主機組進行關聯分析，自動識別風險指數的變化，自動產生告警。 2. 可以和Cisco ISE集成，實現基於用戶的追蹤發現高風險告警 3. 並通過ISE的准入控制，對受影響主機進行隔離阻斷。 |
|---|--|--|



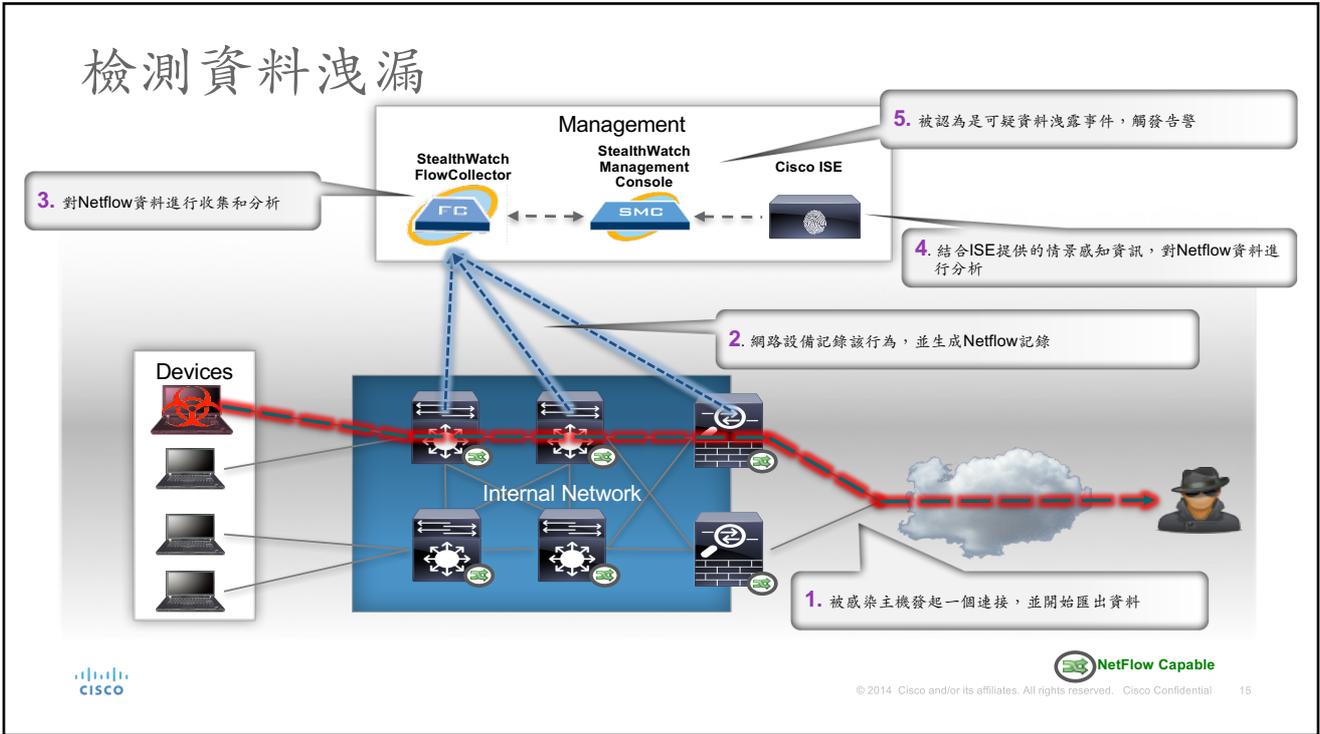
網路行為統計與監控面板



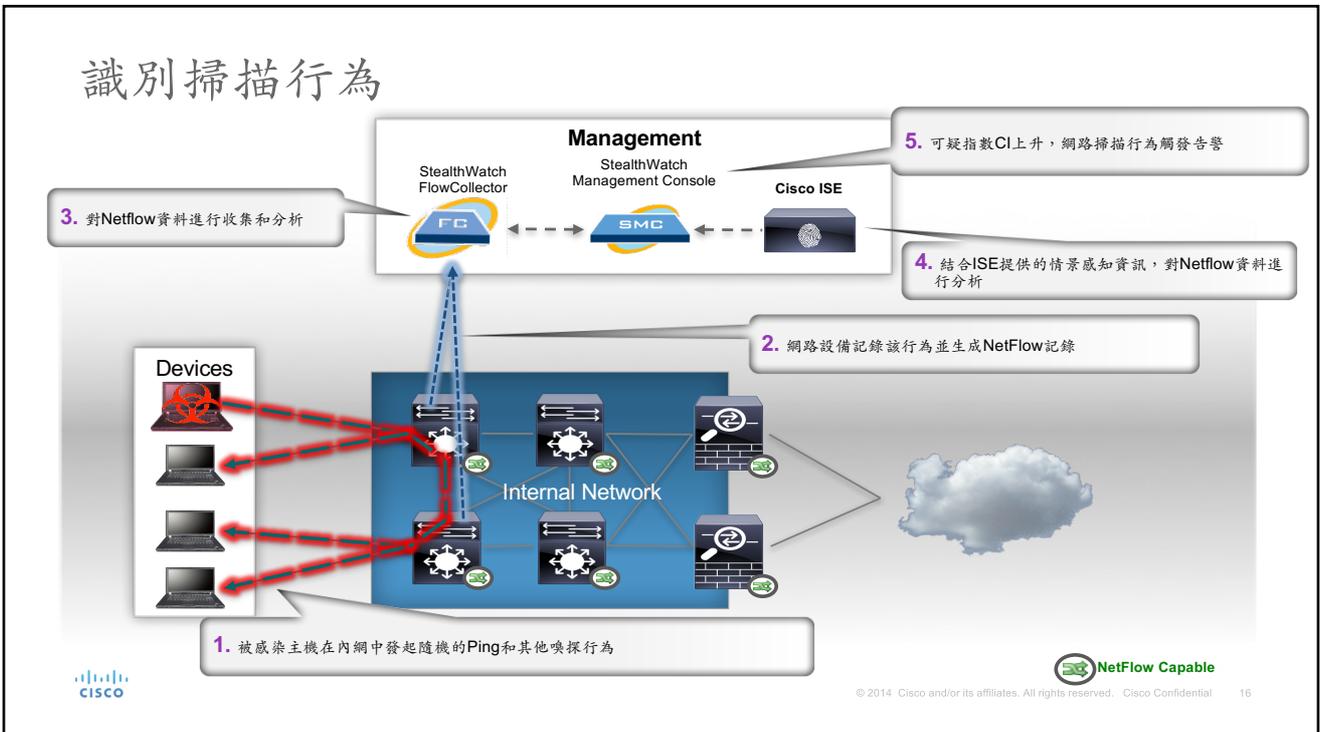
主機組存取關係與監控



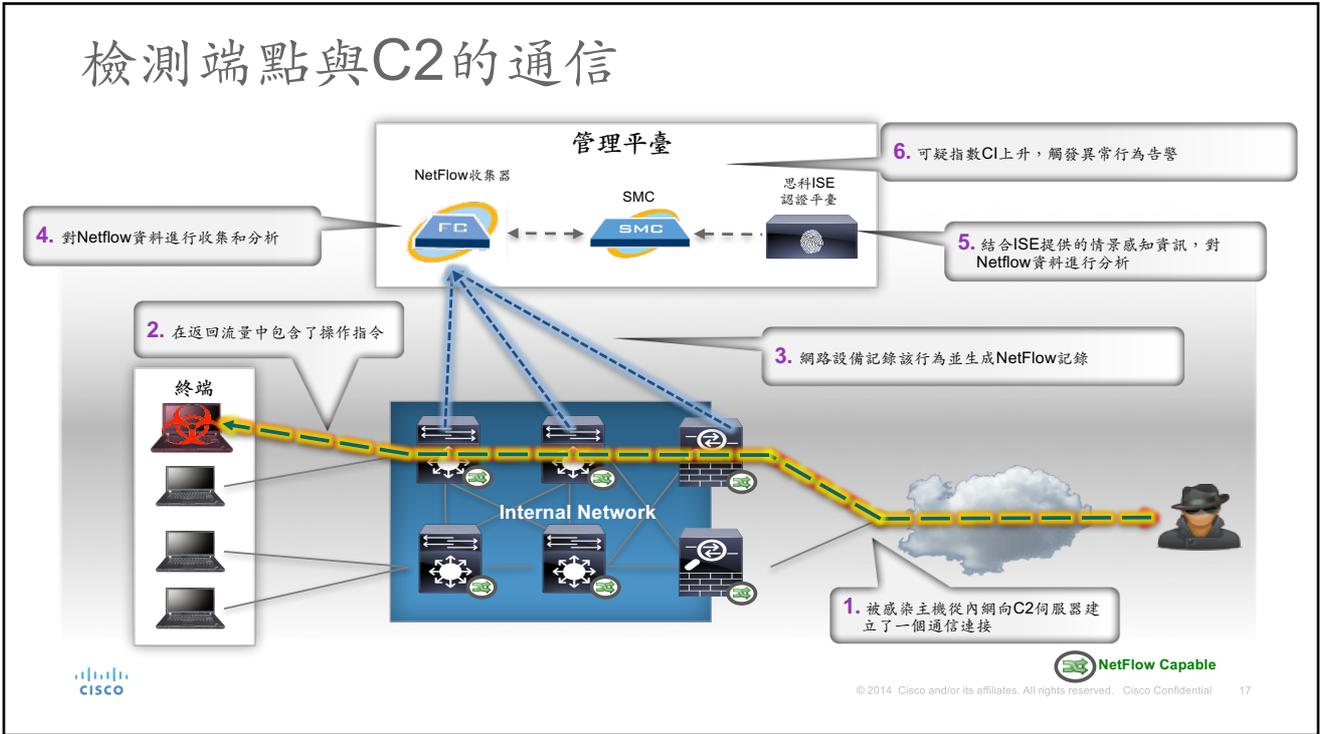
檢測資料洩漏



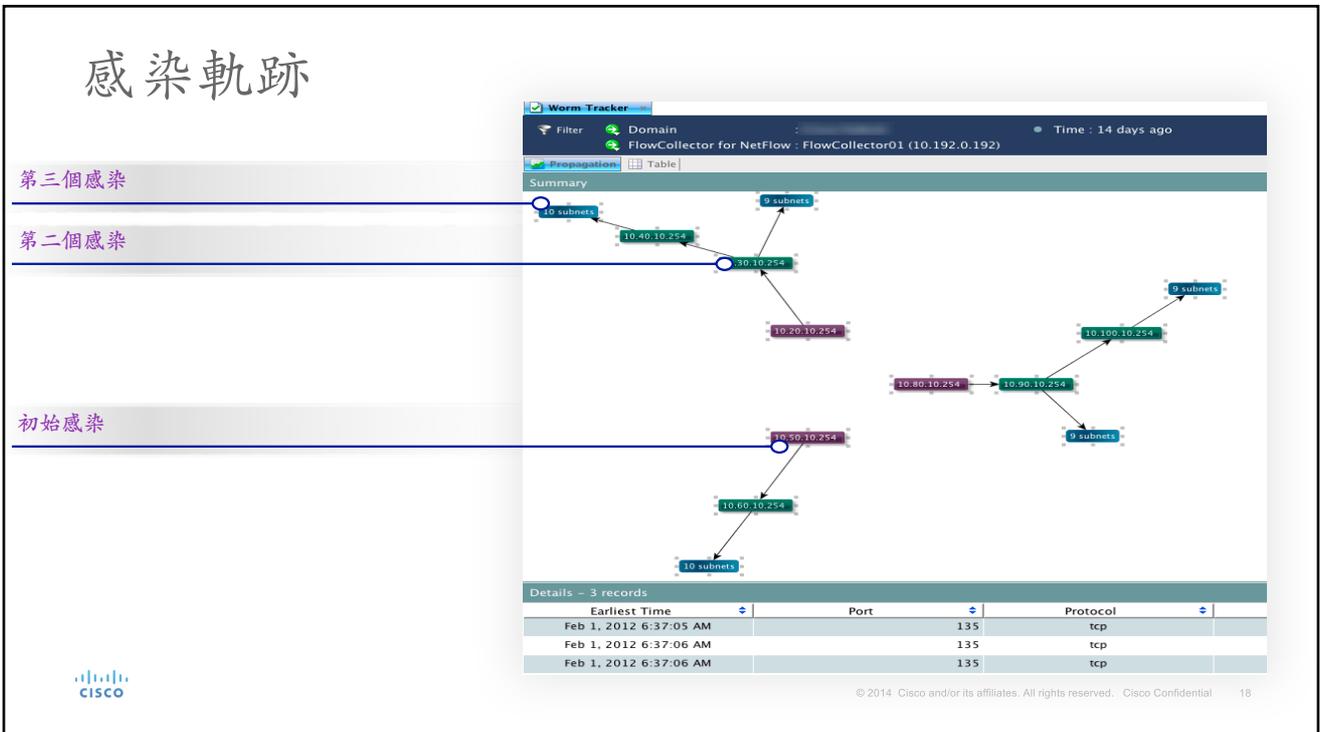
識別掃描行為

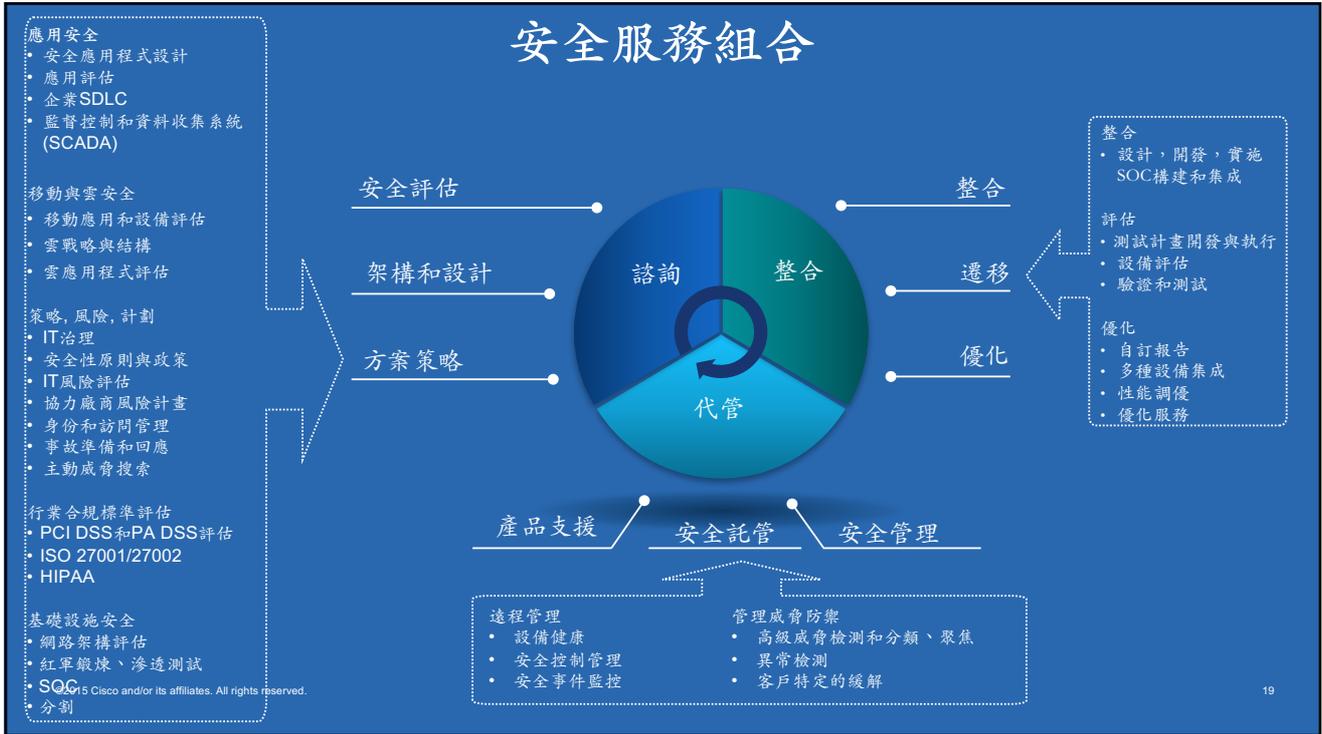


檢測端點與C2的通信



感染軌跡





結論:當網路犯罪成為主流

- 管理預期
 - 確保管理層認識到攻擊的本質是與數位軍備競賽戰鬥
- 建立智慧監測機制
 - 知道要尋找什麼，並建立資訊安全與網路監控機制，以尋找所要尋找之物
- 重新設計IT架構
 - 網路安全分區轉為應用功能型 攻擊者難在網路四處遊蕩從而難以發現最寶貴的資訊
- 實戰的培訓
 - 培訓IT管理者以識別攻擊及防禦知識與手段
- 存取控制權
 - 控制特權使用者的存取
- 情報蒐集與分析
 - 讓情報成為安全戰略的基石 / 分享資訊安全威脅情報

